VULNERABILITY DISCLOSURE POLICY
DATAMOTION, INC.
May 12, 2025

Introduction

DataMotion, Inc. ("**DataMotion**") is committed to ensuring the security of the American public by protecting their information. This Vulnerability Disclosure Policy (the "**Policy**") is intended to give security researchers ("**Researchers**", "**You**", "**Your**") clear guidelines for conducting vulnerability discovery activities and to convey DataMotion's preferences in how to submit discovered vulnerabilities (the "**Report(s)**").

This Policy describes what Systems and Services (defined below), and types of Research (defined below) are covered, how to send DataMotion the Reports, and how long DataMotion asks Researchers to wait before publicly disclosing vulnerabilities.

DataMotion encourages You to Report potential vulnerabilities of its Systems and Services in accordance with this Policy.

Confidentiality

By engaging in Research under this Policy and submitting Your Report to DataMotion, You agree to maintain the confidentiality of all information accessed or discovered during Your Research. This includes, but is not limited to: details of any vulnerabilities found, any data accessed during testing (including sensitive data such as personally identifiable information (PII) of employees or customers, financial information, proprietary information, and trade secrets), details of DataMotion's Systems and Services, and infrastructure, any communications between You and DataMotion regarding vulnerabilities or testing procedures, and any other confidential information (collectively, "**Confidential Information**").

You acknowledge that as part of responsible disclosure, You may eventually publicly disclose details of any vulnerability discovered. However, You agree that You will not publicly disclose any sensitive data (including PII, financial information, or proprietary information) or any other Confidential Information obtained during Your Research. Any such Confidential Information must only be shared with DataMotion and must not be included in any public report or communication. Public disclosure of vulnerabilities may only occur in accordance with the timeline and process outlined in the section of this Policy titled Reporting a Vulnerability.

Authorization

If You make a good faith effort to comply with this Policy during Your Research, Your Research shall be authorized, and DataMotion will collaborate with You to understand and resolve the issue quickly, but in no event longer than the anticipated timeframe set forth under Section Reporting a Vulnerability, and will not recommend or pursue legal action related to Your Research. A good faith effort means conducting Research with the honest intent to comply with all terms of this

Policy, without any intention to cause harm, exploit data, or breach the Policy's guidelines. Actions that exceed the Scope of this Policy, which result in unauthorized access or damage, or otherwise demonstrate negligence or malicious intent will not be considered a good faith effort. If You are unsure whether an action complies with this Policy or is not a good faith effort, or if You have any questions about the Scope of Your Research, You must contact DataMotion at security@datamotion.com before proceeding. Failure to seek clarification when in doubt may be considered non-compliant and not a good faith effort. Should legal action be initiated by a third party against You for activities that were conducted in accordance with this Policy, DataMotion will make this authorization known.

By submitting a Report, You acknowledge that You have read and understood this Policy, and You agree to comply with all its terms and conditions.

Guidelines

Under this Policy, "**Research**" means activities in which You:

- Notify DataMotion as soon as possible after You discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems and services.
- Research shall be provided to DataMotion as described below under the Reporting a Vulnerability section and in no circumstances should a vulnerability be disclosed publicly until advised by DataMotion in writing.
- Do not submit a high volume of low-quality Reports, which are Reports that lack detailed descriptions, clear reproduction steps, or sufficient evidence, making it difficult to understand or verify the vulnerability ("**Low-Quality Reports**").

Once You have established that a vulnerability exists or encounter any sensitive data (including PII, financial information, or proprietary information or trade secrets of any party), **You must stop Your test, notify DataMotion immediately, and not disclose this data to anyone else until DataMotion has said otherwise**.

Test Methods

The following test methods **are not** authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage the Systems and Services, or data;
- Physical testing (e.g., office access, open doors, tailgating), social engineering (e.g., phishing, vishing), or any other non-technical testing;
- Social Engineering;
- SQL Injection;
- Attempting to abuse DataMotion's artificial intelligence chatbot, JenAI Assist (excessive token usage, prompt injection); and
- Attempting to access DataMotion's Systems and Services via DataMotion's cloud provider.

Reporting a Vulnerability

Vulnerabilities should be reported to the DataMotion Vulnerability Submission Form. To ensure DataMotion understands enough about the vulnerability to properly resolve it, it is recommended that Your Report(s) include:

- Describe the location where the vulnerability was discovered and the potential impact of exploitation;
- The type of vulnerability;
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts, error messages, screenshots, and/or code snippets);
- Relevant URLs and/or HTTP requests involved in the vulnerability; and
- Reports should be in the English language, if possible.

Reports may be submitted anonymously. However, DataMotion may request that You provide Your contact information if DataMotion needs to contact You. DataMotion does not support PGP-encrypted emails. By submitting a Report, You acknowledge that You have no expectation of payment and that You expressly waive any future pay claims against DataMotion, and the U.S. Government related to Your submission.

Information submitted under this Policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If Your findings include newly discovered vulnerabilities that affect all users of DataMotion's Systems and Services and not solely DataMotion, DataMotion may share Your Report with the Cybersecurity and Infrastructure Security Agency (CISA), where it will be handled under the CISA's Coordinated Vulnerability Disclosure Process found at: https://www.cisa.gov/coordinated-vulnerability-disclosure-process. DataMotion will not share Your name or contact information without Your express permission.

If You choose to share Your contact information with DataMotion, DataMotion commits to coordinating with You as openly and as quickly as possible, which shall include:

- **Acknowledgement**. Within **seven (7)** business days of receiving a Report from You, DataMotion will acknowledge that Your Report has been received.
- **Transparency**. To the best of DataMotion's ability, it will confirm the existence of the vulnerability to You and be as transparent as possible about what steps are being taken during the remediation process, including on issues or challenges that may delay resolution.
- **Remediation**. DataMotion shall remediate the vulnerability or have a pathway forward for remediation within **sixty (60)** days of receiving Your Report.
- **Disclosure**. Upon receiving notice from DataMotion that the vulnerability has been remediated, You would have the opportunity to publicly disclose such vulnerability, if You chose to do so.

Questions

Questions regarding this Policy may be sent to security@datamotion.com. You are also invited to contact DataMotion with suggestions for improving this Policy.

Document Change History

Version	Date	Description
1.0	May 2025	First Issuance